Strategy And Management · 5 Min Read

Vendor consolidation: What enterprises should consider

Strictly adhering to a well-defined process each time, the number of vendors you work with starts to become irrelevant. Each criterion, or decision factor, will help justify the decision to onboard additional vendors.

ETCIO
Updated On Dec 9, 2021 at 08:28 AM IST

Read by:
1323 Industry Professionals

By Ashish Kaushik

'Vendor consolidation' was recently listed by Gartner as being one of the Top Security and Risk Trends for 2021, after it found 78% of CISOs have 16+ tools in their cybersecurity vendor portfolio. Gartner's 2020 CISO Effectiveness Survey also revealed 12% of CISOs have 46+ tools. Juggling this number of vendors is where lapses can occur and how security may become compromised.

Vendor consolidation is the process of procuring from just a small group of reliable providers, or even a single partner, which can fulfil all or most of your needs. Around 80% of enterprises are leaning towards a consolidation strategy, recognising that if you have fewer vendors to deal with, it follows that managing compliance and security is more straightforward. However, as much as consolidating to a single vendor is the ultimate goal for cost optimization and efficiency, it is very unlikely to happen. Why?

Here’s the problem: no one provider can fulfil or satisfy all security requirements and needs.

For example, a password security tool might be perfect for protecting offline credentials, such as for accessing personal/organization web portals. On the other hand, that same tool might not be the best fit for online cloud resources which need credentials to be auto-rotated. Even for something as fundamental as password protection, an organization may need to source different ‘best-in-class’ solutions from different vendors.

This is just one reason why organizations have ended up procuring from a multitude of vendors. When it comes to cybersecurity, deploying the tools or solutions best suited for the task is surely the right approach, and why multi-vendor strategies are so prevalent. However, using security solutions from many different vendors can introduce additional levels of complexity for most businesses.

Therefore, it’s worth considering both sides of the debate – to consolidate or not to consolidate?

The Pros and Cons of Vendor Consolidation

Advantages of vendor consolidation could be thought of as high-level business efficiency gains. This includes:

- Cost Savings: consolidating products and services from fewer vendors increases ‘buyer power’. In addition, it paves the way for negotiating additional services or larger discounts.
- Time Savings: not only is administration and logistics easier to manage and process, the time required to train staff on multiple tools or platforms is significantly reduced.

- Increased Service and Support: when you work in partnership with fewer vendors, a good relationship can be established, resulting in improved service levels. The larger the portfolio, the vendor will minimize the risk of losing your business.

However, before being lured into what seems to be the most cost-effective approach, you need to consider what you might be missing out on if you exclude certain vendors. Disadvantages of vendor consolidation include:

- Freedom of choice: being limited to a minimum number of vendors, may mean you are not able to use the best tool that suits all your internal requirements. For example, one vendor might provide the best security solution for the DevOps team, but it may not be suited for the Design team.
- Limited Specialization: a chosen vendor may provide a broad spectrum of solutions, but lack the deep expertise required, like a ‘jack of all trades, but master of none’. Without the ability to select an additional vendor that brings a game-changing solution to market, your needs won’t be perfectly met, worse still your security levels may fall behind.
- Dependency: the fewer the vendors, the greater the reliance on their continued success, growth, and existence. Consolidating to a *single* vendor increases the dependency further, and robust security mitigation plans should be in place, in the event of something going wrong.

Vendor Selection Process is Key

If we accept the original problem statement, that no one provider can fulfil or satisfy all security requirements and needs, the multi-vendor approach is probably here to stay. But, in reducing the number CISOs work with, the vendor selection process is key. Rather than rigidly sticking with only one or two chosen vendors, organizations should instead focus on a streamlined process when considering additional vendors. This will include three critical components:

1. Vetting a vendor – what features can they provide? What are the cost implications, both upfront and ongoing? Will they outsource security to a third-party provider?
2. Onboarding a vendor – can their solutions be integrated with the current ecosystem?
3. Off-boarding a vendor – how complicated is it to change vendors? What are the risks when a contract expires? Vendor lock-ins are a particular issue, because when a database is set up in one environment, the process of migrating to a new one can become very complicated.

Fortunately, specialist software is available that supports managing the vendor consolidation and lifecycle process, helping organizations select the most appropriate vendor for their needs. This vendor selection tool allows you to fix minimum selection criteria, such as your organization's customized onboarding process, or compliance requirements, for example, vendors must have ISO certification, or HIPAA competency.

Bottom Line: Strictly adhering to a well-defined process each time, the number of vendors you work with starts to become irrelevant. Each criterion, or decision factor, will help justify the decision to onboard additional vendors.

Conclusion

Vendor consolidation could solve a lot of problems, but realistically there's a long way to go before we can make it a reality in the near future. It's a good strategy to work towards, *provided* a streamlined process is adopted for any new vendor selection. If and when an IT project requires a new and specific cybersecurity configuration, it's imperative to adopt new tools that are fit for purpose, provided it fits within the current ecosystem.

Continuously striving for 'best-in-class' service delivery enables developers to take advantage of the very latest in cybersecurity technology, and not get left-behind if their current vendor(s) cannot provide it. Just like creating the best team requires lots of different people that each bring a particular skill or quality, procuring security solutions via several vendors can create the highest security throughout your infrastructure, services and client solutions. Remember, not all vendors are necessarily the best at everything: when it comes to IT security solutions, one size does not fit all!

The author is CISO, SourceFuse

@2024 ETCIO.com. All Right Reserved.